(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 822 256**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **01 03486**

(51) Int Cl[7] : G 06 F 12/14

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 13.03.01.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 20.09.02 Bulletin 02/38.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *GEMPLUS Société anonyme* — FR.

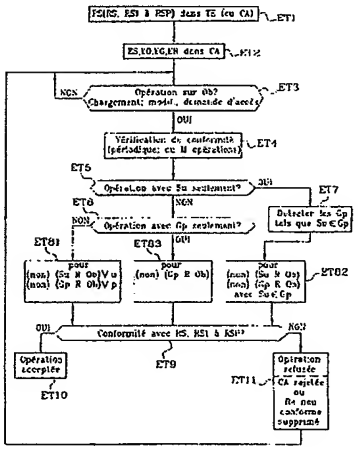
(72) Inventeur(s) : BIDAN CHRISTOPHE et PAULIAC MIREILLE.

(73) Titulaire(s) :

(74) Mandataire(s) :

(54) VERIFICATION DE LA CONFORMITE D'ACCES A DES OBJETS DANS UN SYSTEME DE TRAITEMENT DE DONNEES AVEC UNE POLITIQUE DE SECURITE.

(57) L'invention concerne la conformité de règles d'accès (R) de sujets (Su) à des objets (Ob) avec une politique de sécurité (PS) prédéfinie dans un système de traitement de données de type carte à puce. Chaque règle d'accès définit un droit d'un sujet à accomplir une action sur un objet. La politique de sécurité définit des règles de sécurité (RS) pour l'accès des sujets aux objets. Pour une opération relative à un objet donné (Ob), au moins une règle d'accès relative à l'objet donné est comparée avec les règles de sécurité afin d'accepter l'opération lorsque la règle d'accès est conforme à toutes les règles de sécurité et sinon de refuser l'opération. Une opération peut être un chargement d'objet tel qu'une application, une modification de règles d'accès, ou une suppression ou une adjonction de sujet (s), ou une demande d'accès à l'objet donné par un sujet ou un groupe de sujet.



FR 2 822 256 - A1

2822256

Vérification de la conformité d'accès à des objets dans un système de traitement de données avec une politique de sécurité

La présente invention concerne d'une manière générale la vérification de la conformité de conditions d'accès par des premiers éléments à des deuxièmes éléments avec des règles de sécurité définissant une politique de sécurité. Les premiers éléments sont des sujets constituant des utilisateurs ou modules logiciels d'un moyen de traitement de données. Les deuxièmes éléments sont des objets tels que des applications implémentées dans le moyen de traitement de données. Plus particulièrement, l'invention est relative à des conditions d'accès à des applications implémentées dans une carte à puce, dite également carte à microcontrôleur ou à circuit intégré, qui comporte plusieurs applications relatives à divers services, tels que des applications de commerce électronique, porte-monnaie électronique, service de fidélité, etc.

L'invention est ainsi particulièrement dirigée vers la conformité de toute opération relative à une application dans une carte à puce multi-applicative avec des règles de sécurité. L'opération peut être un chargement ou une modification de l'application, ou des modifications des conditions d'accès à l'application, ou bien encore une demande d'accès à l'application pour accomplir une action sur celle-ci.

La coexistence et la coopération de plusieurs applications au sein d'une même carte à puce soulève de nombreux problèmes du point de vue de la sécurité. En particulier, chaque application possède ses propres données pour lesquelles le fournisseur de

l'application définit des droits d'accès propres à l'application. Les droits d'accès sont des moyens de liaison entre des accès externes qui peuvent être des utilisateurs de la carte ou bien des modules logiciels, comme des interfaces d'usager, et des accès internes à la carte tels que des applications, éventuellement par l'intermédiaire d'autres applications ou d'autres éléments logiciels d'application dans la carte.

Le contrôle des conditions d'accès repose sur l'authentification des sujets, tels que les utilisateurs, qui sont des éléments "actifs" qui manipulent des informations contenues dans des objets, tels que des applications, qui sont des éléments "passifs" contenant des données. Les droits d'accès des sujets aux objets sont régies par des règles de contrôle d'accès entre les sujets et les objets. Chaque règle comporte un droit d'accès, c'est-à-dire un lien entre un sujet et un objet sous la forme d'une action qui peut être accomplie par le sujet sur l'objet.

Il est connu de représenter les droits d'accès de sujets à des objets par une matrice d'accès MA dont les colonnes correspondent à des sujets et dont les lignes correspondent à des objets, comme montré à la figure 1. Par exemple, la matrice MA est relative à trois sujets S1, S2 et S3, tels que trois utilisateurs, et à trois objets O1, O2 et O3, tels que des fichiers et des programmes. Chaque case de la matrice à l'intersection d'une ligne et d'une colonne contient des droits d'accès, c'est-à-dire des actions privilégiées qui peuvent être accomplies par le sujet respectif sur l'objet respectif.

Les droits d'accès peuvent être positifs pour autoriser une action prédéterminée d'un sujet sur un

objet, ou peuvent être négatifs pour interdire une action prédéterminée d'un sujet sur un objet. Par exemple, le sujet S2 peut lire et exécuter l'objet O2 mais ne peut pas écrire dans cet objet, et le sujet S3 peut enregistrer et lire l'objet O3 mais ne peut pas exécuter l'objet O3.

Comme il est connu, les règles de contrôle d'accès sont généralement traitées suivant deux approches.

La première approche consiste en des listes de contrôle d'accès ACL (Access Control List) correspondant aux lignes de la matrice d'accès MA et spécifiant chacune les droits d'accès de sujets à l'objet associé à la ligne. A titre d'exemple, dans une carte à puce multi-applicative du type WINDOWS (marque enregistrée), des listes de contrôle d'accès ACL définissent des accès d'utilisateurs à des fichiers inclus dans la carte.

A l'inverse, la deuxième approche consiste en des capacités correspondant aux colonnes de la matrice MA et spécifiant chacune les droits d'accès du sujet associé à la colonne sur les objets. Par exemple, le contrôle d'accès porte sur des méthodes d'applets pour cartes à puce multi-applicatives de type JavaCard dans lesquelles des programmes en langage Java ont été écrits. Les capacités sont sous la forme de pointeurs permettant d'effectuer des appels à des objets, dans des applets prédéterminés constituant des sujets.

Dans le domaine de la carte à microcontrôleur, la notion de politique de sécurité est généralement omise. En effet, les cartes étant jusqu'alors généralement mono-applicatives, ceci impose une unique politique de sécurité de taille raisonnable

pour assurer que les droits d'accès correspondent bien au souhait du développeur ayant en charge la définition des droits d'accès.

Comme déjà précisé, les droits d'accès sont exprimés sous la forme de règles de contrôle d'accès. Il faut alors vérifier et garantir que les droits d'accès sont complets et consistants vis-à-vis d'une politique, c'est-à-dire qu'ils offrent au moins deux propriétés, la complétude et la consistance. La complétude de droit d'accès assure que pour tout sujet et tout objet, il existe au moins un droit d'accès spécifiant si le sujet est autorisé ou non à accéder à l'objet. La consistance des droits d'accès garantit que pour tout sujet et tout objet, si plusieurs droits d'accès à l'objet sont définis, les droits d'accès spécifient tous le même type de droit positif ou négatif. La complétude des droits d'accès vis-à-vis d'une politique de sécurité assure que les droits d'accès définissent tous les droits spécifiés par la politique de sécurité. La consistance des droits d'accès vis-à-vis d'une politique assure que les droits d'accès sont limités à ceux définis par la politique de sécurité et ne définissent pas plus de droits.

Actuellement dans les cartes multi-applicatives, les propriétés de complétude et de consistance des droits d'accès avec une politique de sécurité ne peuvent pas être vérifié. Le développeur en charge de la définition des droits d'accès n'est donc pas en mesure de vérifier que les droits d'accès spécifiés correspondent aux règles de la politique de sécurité souhaitée.

L'introduction de cartes multi-applicatives complexifie le problème de la coexistence de plusieurs applications et donc la coexistence de

plusieurs politiques de sécurité, la coopération entre les applications augmentant encore la complexité des politiques.

La présente invention a pour objectif de fournir un procédé pour vérifier la conformité des droits d'accès de plusieurs sujets à plusieurs objets, tels que des applications dans une carte multi-applicative, avec une politique de sécurité globale qui est mise en oeuvre par le gestionnaire de la carte qui peut être une personne différente du développeur de chacune des applications. Ce procédé garantit ainsi la complétude et la consistance des droits d'accès vis-à-vis d'une politique de sécurité : les droits d'accès définissent tous les droits spécifiés par la politique de sécurité selon la propriété de complétude, et se limitent à ces droits de politique de sécurité selon la propriété de consistance.

Pour atteindre cet objectif, un procédé pour vérifier un ensemble de règles d'accès de premiers éléments à des deuxièmes éléments dans un système de traitement de données, chaque règle définissant un droit d'un premier élément à accomplir une action sur un deuxième élément, est caractérisé en ce qu'il comprend, une définition de règles de sécurité pour l'accès des premiers éléments aux deuxièmes éléments, et pour chaque opération relative à un deuxième élément donné, une comparaison d'au moins une règle d'accès donnée au deuxième élément donné avec les règles de sécurité de manière à accepter l'opération lorsque la règle d'accès est conforme à toutes les règles de sécurité et à signaler la non conformité de

l'opération lorsque la règle d'accès n'est pas conforme à l'une des règles de sécurité.

Comme on le verra dans la suite, les premiers éléments sont par exemple des sujets tels que des utilisateurs, et les deuxièmes éléments sont par exemple des objets, tels que des applications dans une carte à puce multi-applicative incluse dans le système de traitement de données.

Selon une première réalisation, le système de traitement de données comprend un objet électronique portable dans lequel au moins les deuxièmes éléments sont implantés, et un moyen de sécurité externe à l'objet électronique portable dans lequel les règles de sécurité sont implantées et qui effectue la comparaison.

Selon une deuxième réalisation, le système de traitement de données est un objet électronique portable dans lequel au moins les deuxièmes éléments et les règles de sécurité sont implantés et qui effectue la comparaison.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs réalisations préférées de l'invention en référence aux dessins annexés correspondants dans lesquels :

- la figure 1 est un diagramme montrant une matrice de contrôle entre trois sujets et trois objets, déjà commentée selon la technique antérieure ;

- la figure 2 est un bloc-diagramme schématique d'un système de traitement de données pour la mise en oeuvre du procédé de contrôle de conformité selon une première réalisation de l'invention ; et

- la figure 3 est un algorithme du procédé de vérification de conformité selon l'invention.

Un système électronique de traitement de données tel qu'illustré à la figure 2 comprend un objet électronique portable telle qu'une carte à puce CA et un terminal TE doté d'un clavier CL et d'un lecteur LE pour lire les données dans la carte. La "puce" de la carte CA est un microcontrôleur comportant un microprocesseur PR et trois mémoires MO, MNV et MA. La mémoire MO de type ROM inclut un système d'exploitation OS de la carte. La mémoire MNV est une mémoire non volatile de type programmable et effaçable, comme une mémoire EEPROM. La mémoire MNV contient des données notamment liées au possesseur et au fournisseur de la carte et en particulier des applications AP constituant des objets au sens de l'invention et des données liées aux accès aux applications AP, telles que des règles d'accès R et des sujets Su. La mémoire MA est de type RAM et destinée à recevoir notamment des données du terminal TE de la carte. Tous les composants PR, MO, MNV et MA sont reliés entre eux par un bus interne BU. Lorsque la carte CA est introduite dans le lecteur LE du terminal TE, le bus BU est relié au terminal TE à travers une liaison de contacts LI lorsque la carte est du type à contacts électriques.

Selon cette première réalisation, une politique de sécurité définie par des règles de sécurité RS relative à toutes les applications AP dans la carte à puce CA est pré-mémorisée dans le terminal TE. Par exemple, le terminal TE appartient au distributeur de la carte à puce qui peut être différent de chaque développeur d'application ayant en charge la

définition de règles d'accès à au moins une application respective.

En variante, le terminal contenant les règles de sécurité et vérifiant la conformité des règles d'accès avec les règles de sécurité est un serveur relié par un réseau de télécommunication à un terminal d'accueil de la carte à puce.

Selon une deuxième réalisation, au lieu que la politique de sécurité PS soit implantée dans le terminal TE, les règles de sécurité RS définissant la politique de sécurité sont implantées dans la mémoire ROM MO de la carte à puce CA qui constitue le système de traitement de données.

La description ci-après du procédé de vérification de conformité selon l'invention est valable indifféremment pour ces deux réalisations présentées ci-dessus.

Les réalisations décrites ci-après du procédé de vérification de conformité d'accès de sujets à des objets avec une politique de sécurité se réfèrent aux cinq ensembles suivants :

- un ensemble d'objet EO = {O1, ... Ob, ... OB} avec $1 \leq b \leq B$,
- un ensemble de sujet ES = {S1, ... Su, ... SU} avec $1 \leq u \leq U$ relatif à des sujets ayant chacun au moins un accès à un objet donné Ob,
- un ensemble de groupe de sujet EG ={G1, ... Gp, ... GP} relatif à des sujets ayant chacun au moins un accès à l'objet Ob, un sujet dans un groupe ayant tous les droits d'accès accordés à ce groupe, et un sujet pouvant appartenir à un ou plusieurs groupes,
- un ensemble de règle de droit d'accès ER = {R1, ... Re, ... RE} avec $1 \leq e \leq E$ régissant l'accès

des sujets de l'ensemble ES et des groupes de l'ensemble EG à l'objet donné Ob, et

- un ensemble de règles de sécurité RS applicables à tous les sujets de l'ensemble donnant accès à l'objet Ob et de règles de sécurité RS1 à RSP applicables respectivement aux groupes G1 à GP pour accéder à l'objet Ob.

Si R (ou RS) désigne un droit, c'est-à-dire une action telle que lecture, écriture, exécution ou enregistrement, qui peut être accomplie par un sujet quelconque Su sur un objet donné quelconque Ob, le contrôle d'accès est régi par les règles de droit positif suivantes :

- (SuROb) : le sujet Su a le droit R sur l'objet Ob, c'est-à-dire est autorisé à accomplir l'action R sur l'objet donné Ob ;

- (GpROb) : les sujets du groupe Gp ont le droit R sur l'objet Ob ;

ainsi que par les règles de droit négatif suivantes :

- non(SuROb) : le sujet Su n'a pas le droit R sur l'objet donné Ob, c'est-à-dire est interdit d'accomplir l'action R sur l'objet Ob ;

- non(GpROb) : les sujets du groupe Gp n'ont pas le droit R sur l'objet Ob.

Dans la suite, on appellera "droit direct" du sujet Su sur l'objet Ob, un droit obtenu directement par la règle (SuROb), c'est-à-dire sans passer par l'intermédiaire d'un groupe ; et "droit indirect" du sujet Su sur l'objet Ob, un droit obtenu par la règle (GpROb) à travers un groupe Gp dans lequel est inclus le sujet Su.

En référence maintenant à la figure 3, le procédé de vérification de conformité comprend principalement des étapes ET1 à ET8.

Au début du procédé, une première étape initiale ET1 définit une politique de sécurité PS qui comporte des règles de sécurité RS qui sont communes à tous les objets O1 à OB de l'ensemble EO ainsi que des règles de sécurité respectivement pour des groupes de sujet prédéterminés et des objets prédéterminés, et en particulier pour les groupes G1 à GP associés à l'objet donné Ob. La politique de sécurité est implantée dans le terminal TE, ou dans la mémoire MNV de la carte à puce CA.

La deuxième étape initiale ET2 définit les quatre groupes ES, EO, EG et ER pour les implémenter dans les mémoires MO et MNV de la carte à puce CA.

L'étape suivante ET3 concerne le déclenchement d'une opération sur l'objet donné Ob. Cette opération peut être le chargement de l'objet donné Ob, par exemple en tant que nouvelle application, dans la mémoire EEPROM MNV de la carte CA, y compris les règles d'accès propres à l'application définies à une étape antérieure ET2 et écrites dans la mémoire MNV, ou une modification de règle d'accès relative à l'objet donné Ob. La modification de règle d'accès peut être une suppression ou une adjonction d'une règle d'accès relative à un sujet Su ou un groupe Gp et naturellement à l'objet donné Ob. L'opération sur l'objet donné Ob peut être simplement une demande d'accès de droit à l'objet donné par un sujet Su ou un groupe Gp du type (SuROb) ou (GpROb), ou une modification d'un ou de plusieurs sujets ou d'un groupe ayant un accès sur l'objet donné Ob, c'est-à-dire une suppression ou une adjonction d'un ou de plusieurs sujets ou d'un groupe.

La vérification de conformité proprement dite par comparaison de règles d'accès relatives à l'objet

donné Ob à toutes les règles de sécurité débute à l'étape ET4. En variante, cette vérification de conformité est effectuée périodiquement par exemple toutes les vingt quatre heures lorsque la carte à puce CA est utilisée, ou bien toutes les M opérations relatives à l'objet donné Ob, où M désigne un entier au moins égal à 2.

D'une manière générale, selon une première réalisation, toutes les règles d'accès positives et négatives Re relatives à l'objet donné Ob et à un quelconque sujet Sq pour un droit direct ou à un quelconque groupe Gp pour un droit indirect ont leur conformité vérifiée par rapport à toutes les règles de sécurité RS et RSp quel que soit l'indice p défini par la politique de sécurité pour l'objet Ob, comme indiqué à des étapes ET81, ET82, ET83 et ET9 qui succèdent alors directement à l'étape ET4 à travers une réponse négative à l'étape intermédiaire ET6 ou après l'étape ET7. En pratique, la vérification de la conformité d'une règle d'accès résulte d'une comparaison de cette règle avec chacune des règles de sécurité. Par exemple, une règle de sécurité commune à tous les sujets et tous les groupes relatifs à l'objet Ob peut être une interdiction d'écrire dans l'objet Ob, et une règle de sécurité RSp pour le groupe Gp peut être une autorisation de lire l'objet donné Ob par tous les sujets appartenant au groupe Gp.

Cependant, selon d'autres réalisations, le procédé distingue des opérations relatives seulement à un sujet Su, comme une demande d'accès direct du sujet Su à l'objet Ob ou une adjonction du sujet Su, à l'étape ET5, et une opération relative seulement à un groupe donné Gp, comme une demande d'accès de droit indirect à l'objet donné Ob ou un ajout ou

suppression de sujet ou une modification de droit relative au groupe Gp, comme indiqué à l'étape ET6. Si aucune des conditions des étapes ET5 et ET6 n'est satisfaite, le procédé passe directement de l'étape ET4 à l'étape ET81 déjà commentée.

Lorsque l'opération est relative seulement à un sujet Su et à l'objet Ob, l'étape ET5 est suivie d'une étape ET7 au cours de laquelle tous les groupes Gp qui contiennent le sujet Su sont détectés. Dans cette réalisation, l'étape ET81 est remplacée par l'étape ET82 qui vérifie la conformité de toutes les règles d'accès positives et négatives relatives à l'objet donné Ob et directement au sujet Su ou indirectement aux groupes Gp contenant le sujet Su. Ces règles d'accès sont comparées à toutes les règles de sécurité communes RS et aux règles de sécurité RS1 à RSp et en particulier relatives au groupe Gp à l'étape ET9. Par l'intermédiaire des étapes ET7 et ET82, le procédé vérifie ainsi que la capacité d'un sujet Su relative à l'objet donné Ob est conforme à la politique de sécurité PS.

Lorsque l'opération sur l'objet donné Ob est relative seulement à un groupe de sujet Gp à l'étape ET6, toutes les règles de droit d'accès de type positif (GpROb) et négatif non(GpROb) ont leur conformité vérifiée par comparaison avec toutes les règles de sécurité communes RS et les règles de sécurité RS1 à RSp relatives à tous les groupes, et particulièrement relatives au groupe donné Gp, à une étape ET83. A travers les étapes ET6 et ET83, le procédé vérifie ainsi que la liste de contrôle d'accès concernant tous les droits d'accès des sujets dans un groupe donné Gp est en conformité avec la politique de sécurité PS.

Si après l'étape ET81, ou ET82 ou ET83, les règles d'accès comparées sont bien conformes aux règles de sécurité, l'opération demandée à l'étape ET3 est acceptée à l'étape ET10, et le procédé revient à l'étape ET3 pour une vérification de conformité relative à une autre opération sur l'objet Ob, ou à une opération sur un autre objet.

En revanche, si au moins l'une des règles de droit d'accès comparées et définies à l'une des étapes ET81, ET82 et ET83 n'est pas conformes avec l'une des règles de sécurité à l'étape ET9, l'étape ET11 refuse l'opération demandée à l'étape ET3, et le procédé revient ensuite à l'étape ET3. Le refus de l'opération demandée à l'étape ET11 peut être accompagné d'un rejet de la carte à puce CA, ou d'une suppression de la ou des règles de droit d'accès qui n'étaient pas conformes aux règles de sécurité.

A titre d'exemple, il est supposé qu'un premier groupe G1 composé de sujets S1 et S2 ne possède que le droit d'accès en lecture sur l'objet donné Ob, un deuxième groupe G2 composé de sujets S2 et S3 ne possède que le droit d'accès en écriture sur l'objet Ob, et que les deux groupes G1 et G2 sont autorisés à exécuter l'objet Ob tel qu'une application. Par ailleurs, l'étape ET1 définit deux règles de sécurité RS1 et RS2. Selon la première règle RS1, le groupe G1 n'est pas autorisé à écrire sur les objets de l'ensemble EO, et donc y compris sur l'objet donné Ob. Selon la deuxième règle de sécurité RS2, le groupe G2 n'est pas autorisé à lire les objets de l'ensemble EO.

Pour cet exemple, les étapes ET6 et ET83 du procédé selon la figure 3 sont effectuées. Une demande d'accès en lecture du groupe G1 fait

apparaître à l'étape ET9 une conformité pour le sujet S1 appartenant seulement au groupe G1 entre la règle d'accès en lecture du groupe G1 et la règle de sécurité en interdiction d'écriture du groupe G1, et une conformité pour le sujet S3 entre la règle de droit d'accès en écriture du groupe G2 et la règle de sécurité d'interdiction en lecture du groupe G2. Par contre, l'étape ET9 signale un défaut de conformité pour le sujet S2 qui appartient à la fois aux groupes G1 et G2. Pour le sujet S2 la règle de droit d'accès en lecture relative au groupe G1 n'est pas conforme à la règle de sécurité d'interdiction en lecture pour le groupe G2, et la règle de droit d'accès en écriture pour le groupe G2 n'est pas conforme avec la règle de sécurité d'interdiction en écriture du groupe G1. L'étape ET11 procède alors à la suppression des droits d'accès en lecture et écriture du sujet S2 qui ne conserve que le droit d'accès en exécution en commun avec les autres sujets S1 et S3.

Bien que la figure 3 soit relative à la conformité d'opérations sur un objet donné Ob, d'une manière plus générale, toute opération relative à l'un quelconque des objets O1 à OB de l'ensemble EO peut provoquer une vérification de conformité générale de toutes les listes de contrôle d'accès et capacités relatives à tous les objets O1 à OB par rapport à toutes les règles de sécurité de la politique de sécurité. Une telle vérification de conformité générale est de préférence réalisée au moins lors de la mise en service et la personnalisation de la carte à puce CA.

REVENDICATIONS

1 - Procédé pour vérifier la conformité de règles d'accès (Re) définissant respectivement des droits autorisant et/ou interdisant des premiers éléments (Su), tels que des utilisateurs, à accomplir des actions sur des deuxièmes éléments (Ob), tels que des applications implantées dans un objet électronique portable (CA), avec des règles de sécurité (RS) limitant les règles d'accès des premiers éléments aux deuxièmes éléments, caractérisé en ce qu'il comprend, pour chaque opération (ET3) relative à un deuxième élément donné (Ob), telle que notamment un chargement du deuxième élément donné (Ob) ou une modification de règle d'accès relative au deuxième objet donné dans l'objet électronique portable (CA), une comparaison (ET81, ET82, ET83, ET9) d'au moins une règle d'accès (Su/GpRObb) au deuxième élément donné avec les règles de sécurité (RS) de manière à accepter (ET10) l'opération lorsque ladite règle d'accès (R) est conforme à toutes les règles de sécurité et à signaler la non conformité de l'opération lorsque ladite règle d'accès n'est pas conforme à l'une des règles de sécurité.

2 - Procédé conforme à la revendication 1, selon lequel ladite opération (ET3) est ou une suppression ou une adjonction d'une règle d'accès (R) relative au deuxième élément donné, ou une suppression ou une adjonction d'un premier élément (Su) ou de plusieurs premiers éléments (Gp) ayant accès à l'objet donné (Ob), ou une demande d'accès à l'objet donné (Ob) par un premier élément (Su) ou par un groupe (Gp) de premier élément.

3 - Procédé conforme à la revendication 1, selon lequel, lorsque l'opération (ET5) est relative seulement à un premier élément donné (Su) et au deuxième élément donné (Ob), la comparaison (ET82) consiste à comparer toutes les règles d'accès (SuROb, Gp(Su)ROb) relatives au premier élément donné (Su) et au deuxième élément donné (Ob) avec toutes les règles de sécurité (RS).

4 - Procédé conforme à la revendication 1, selon lequel certains des premiers éléments appartiennent chacun à un ou plusieurs groupes de premier élément (Gp), un premier élément dans un groupe ayant tous les droits d'accès accordés au groupe, caractérisé en ce que, lorsque l'opération (ET6) est relative à un groupe donné de premier élément (Gp), la comparaison (ET83) consiste à comparer toutes les règles d'accès (GpROb) relatives au groupe donné et au deuxième élément donné (Ob) avec toutes les règles de sécurité (RS).

5 - Procédé conforme à une quelconque des revendications 1 à 4, selon lequel la comparaison (ET81, ET82, ET83, ET9) est effectuée périodiquement.

6 - Procédé conforme à une quelconque des revendications 1 à 5, selon lequel les règles de sécurité (RS) sont implantées dans un moyen de sécurité (TE) qui est externe à l'objet électronique portable (CA) et qui effectue la comparaison (ET81, ET82, ET83, ET9).

7 - Procédé conforme à une quelconque des revendications 1 à 5, selon lequel les règles de sécurité (RS) sont implantées dans l'objet

électronique portable (CA) qui effectue la comparaison (ET81, ET82, ET83, ET9).

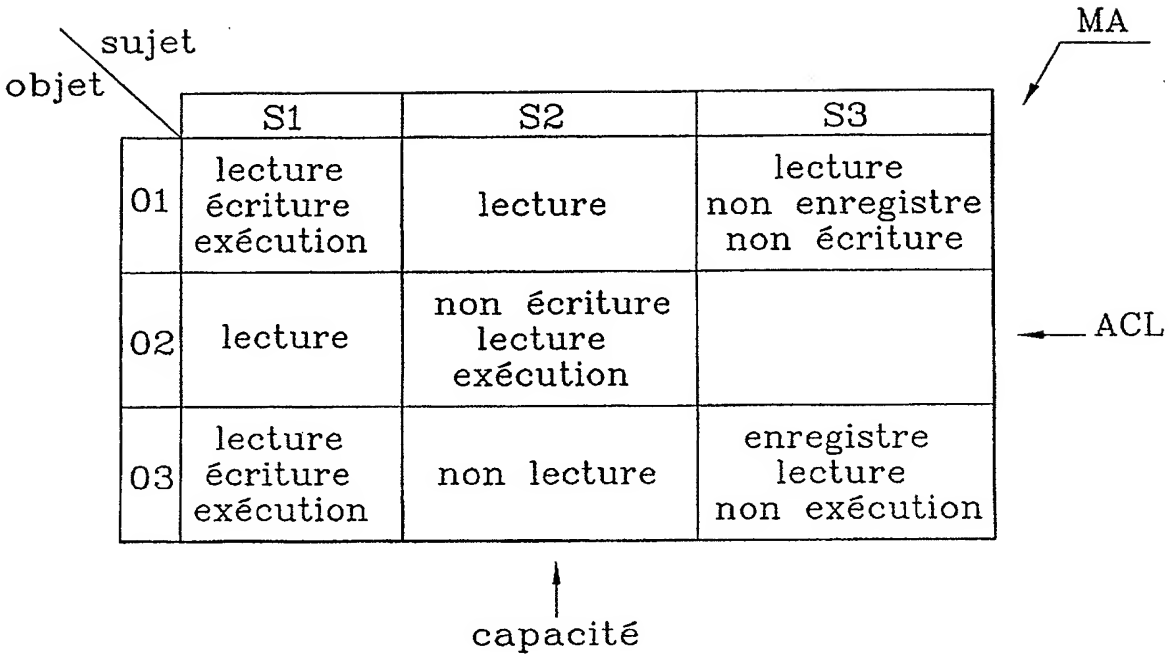

sujet
objet
MA
S1
S2
S3
01
lecture
écriture
exécution
lecture
lecture
non enregistre
non écriture
02
lecture
non écriture
lecture
exécution
ACL
03
lecture
écriture
exécution
non lecture
enregistre
lecture
non exécution
capacité

Fig. 1

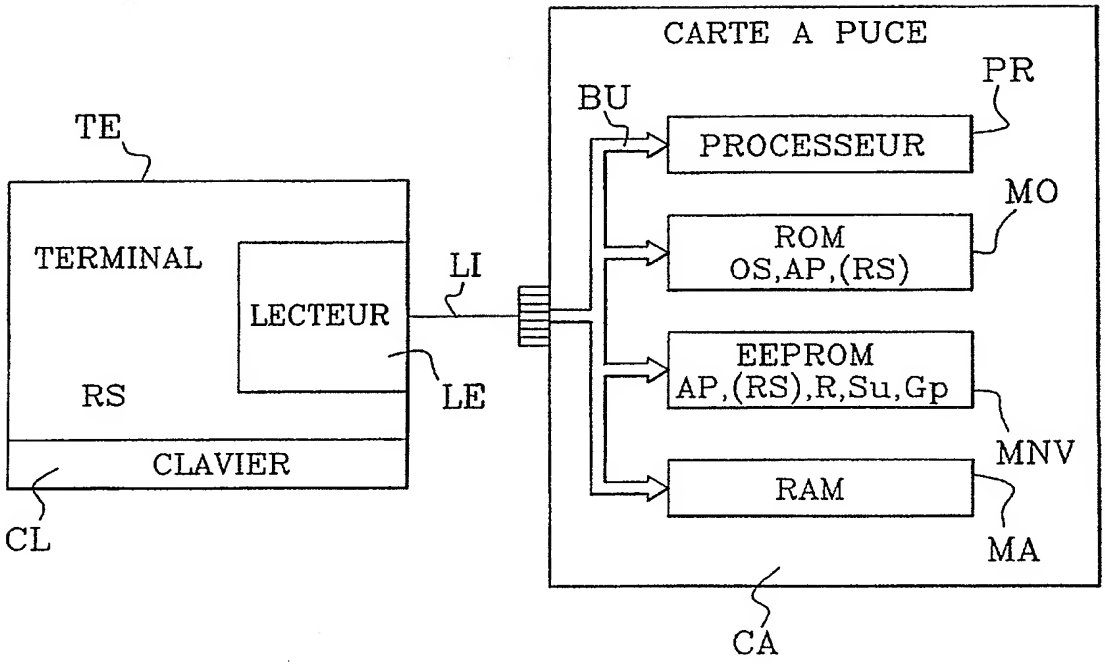

CARTE A PUCE
PR
BU
PROCESSEUR
MO
ROM
OS,AP,(RS)
EEPROM
AP,(RS),R,Su,Gp
MNV
RAM
MA
CA
TE
TERMINAL
LECTEUR
LI
LE
RS
CLAVIER
CL

Fig. 2

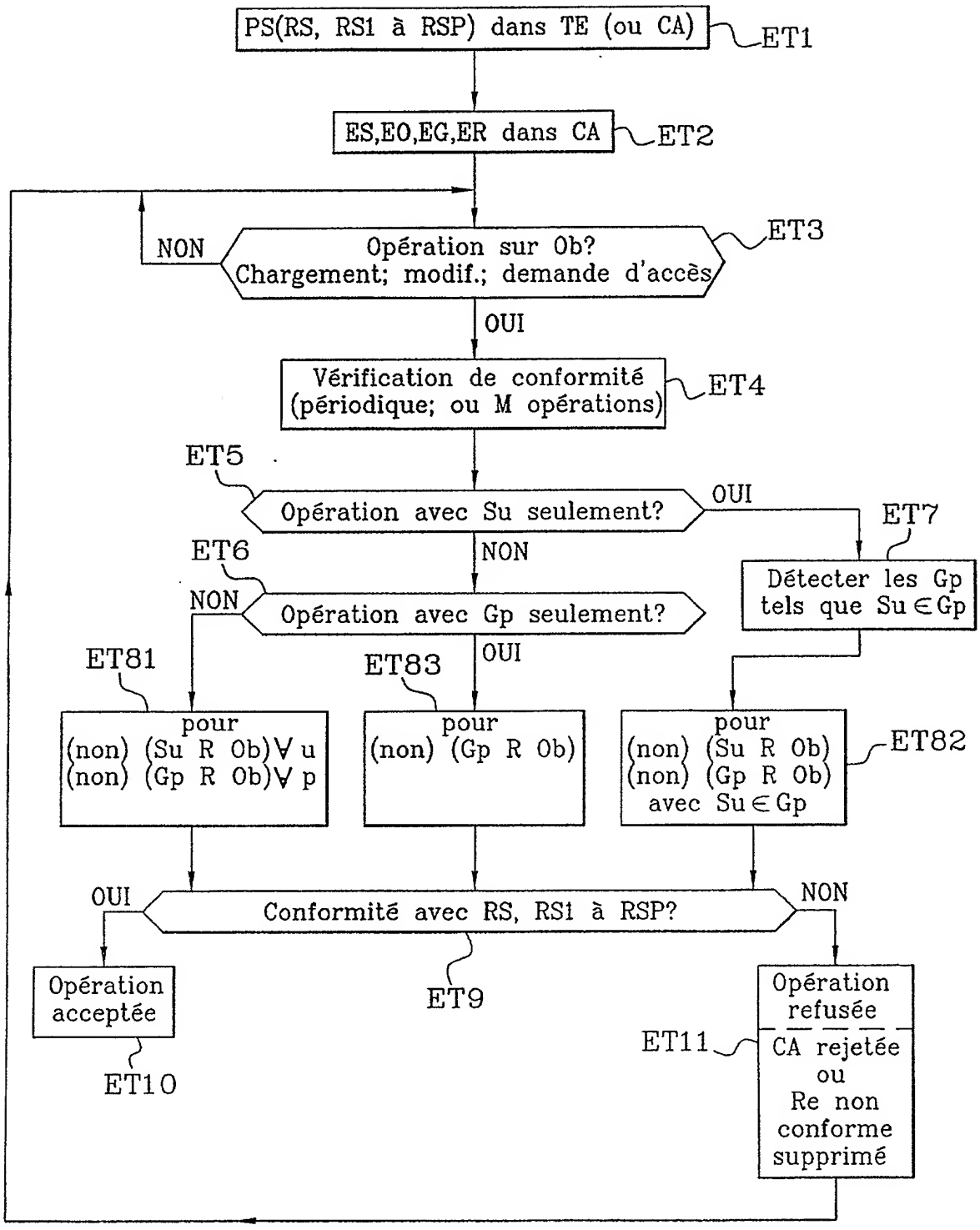

PS(RS, RS1 à RSP) dans TE (ou CA)
ET1
ES,EO,EG,ER dans CA
ET2
NON
Opération sur Ob?
Chargement; modif.; demande d'accès
ET3
OUI
Vérification de conformité
(périodique; ou M opérations)
ET4
ET5
Opération avec Su seulement?
OUI
ET7
NON
ET6
NON
Opération avec Gp seulement?
Détecter les Gp
tels que Su ∈ Gp
ET81
ET83
OUI
pour
(non) (Su R Ob)∀ u
(non) (Gp R Ob)∀ p
pour
(non) (Gp R Ob)
pour
(non) (Su R Ob)
(non) (Gp R Ob)
avec Su ∈ Gp
ET82
OUI
Conformité avec RS, RS1 à RSP?
NON
Opération
acceptée
ET10
ET9
Opération
refusée
ET11
CA rejetée
ou
Re non
conforme
supprimé

Fig. 3

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2822256

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 604190
FR 0103486

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	WO 92 13322 A (GEMPLUS CARD INTERNATIONAL) 6 août 1992 (1992-08-06) * abrégé; revendications; figures 1-5 * * page 24, ligne 18 - page 25, ligne 22 *	1	G06F12/14
A	FR 2 687 816 A (GEMPLUS CARD INTERNATIONAL) 27 août 1993 (1993-08-27) * abrégé; revendications; figure 1 * * page 7, ligne 32 - page 8, ligne 27 *	1	
A	WO 97 44762 A (GEMPLUS) 27 novembre 1997 (1997-11-27) * abrégé; revendications; figures *	1	
A	US 5 220 604 A (M. GASSER) 15 juin 1993 (1993-06-15)		

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

G07F
G06F

Date d'achèvement de la recherche	Examinateur
17 janvier 2002	David, J

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0103486 FA 604190

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 17-01-2002
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 9213322	A	06-08-1992	FR	2673476 A1	04-09-1992
			DE	69205425 D1	16-11-1995
			DE	69205425 T2	21-03-1996
			EP	0589884 A1	06-04-1994
			ES	2082451 T3	16-03-1996
			WO	9213322 A1	06-08-1992
			JP	6504862 T	02-06-1994
			US	5473690 A	05-12-1995
FR 2687816	A	27-08-1993	FR	2687816 A1	27-08-1993
			EP	0565389 A1	13-10-1993
WO 9744762	A	27-11-1997	FR	2748834 A1	21-11-1997
			AU	718446 B2	13-04-2000
			AU	3035797 A	09-12-1997
			CA	2255593 A1	27-11-1997
			EP	0906603 A1	07-04-1999
			FR	2748880 A1	21-11-1997
			WO	9744762 A1	27-11-1997
			JP	2000510977 T	22-08-2000
			US	6216014 B1	10-04-2001
US 5220604	A	15-06-1993	AUCUN		

EPO FORM P0465